

UNCLASSIFIED

16 November 2015



NORTH DAKOTA

Critical Infrastructure and Key Resources (CI/KR) Ticker



The North Dakota Open Source (CI/KR) Ticker a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the (CI/KR) Ticker to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The (CI/KR) Ticker is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

TABLE OF CONTENTS

<u>North Dakota</u>	3
<u>Regional</u>	3
<u>National</u>	3
<u>International</u>	4
<u>Banking and Finance Industry</u>	5
<u>Chemical and Hazardous Materials Sector</u>	6
<u>Commercial Facilities</u>	6
<u>Communications Sector</u>	7
<u>Critical Manufacturing</u>	8
<u>Defense/ Industry Base Sector</u>	8
<u>Emergency Services</u>	8
<u>Energy</u>	9
<u>Food and Agriculture</u>	9
<u>Government Sector (including Schools and Universities)</u>	10
<u>Information Technology and Telecommunications</u>	10
<u>Public Health</u>	12
<u>Transportation</u>	12
<u>Water and Dams</u>	13
<u>North Dakota Homeland Security Contacts</u>	14

NORTH DAKOTA

(National) Cloverdale Foods Company recalls beef and pork product due to misbranding and undeclared allergen. Mandan, North Dakota-based Cloverdale Foods Company issued a voluntary recall November 7 for 5,208 pounds of beef and pork jalapeno cheddar bratwurst products after a store audit discovered that the products were incorrectly labeled as beef frankfurters and contained undeclared milk allergens. Products were sold to three distributors and shipped nationwide. <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-139-2015-release>

REGIONAL

(Minnesota) USDA awards millions for rural electric infrastructure. The U.S. Department of Agriculture Development State Director in Minnesota announced November 5 that nearly \$222 million in loans will be distributed to 16 utilities and cooperatives throughout the State to build and improve 12,000 miles of electrical distribution and transmission lines in rural communities. http://www.mankatofreepress.com/news/local_news/usda-awards-millions-for-rural-electric-infrastructure/article_3c926c18-8333-11e5-87b5-5f343c648cde.html

NATIONAL

(National) Governors of Michigan, Alabama reject resettlement of Syrian refugees in their states. The terrorist attacks in Paris have prompted two governors to announce that Syrian refugees will not be allowed to resettle in their states. By Monday afternoon, seven governors across the country said they would refuse Syrian refugees. <https://www.washingtonpost.com/news/morning-mix/wp/2015/11/16/governors-of-michigan-alabama-reject-resettlement-of-syrian-refugees-in-their-states/>

(National) U.S. President quashes Keystone XL in bid to boost climate leverage. The U.S. President announced November 6 that he sided with the U.S.

UNCLASSIFIED

Department of State and voted against the proposed Keystone XL pipeline, claiming that the pipeline would not advance U.S. interests and would have undercut efforts towards a global climate change deal.

<http://news.yahoo.com/ap-sources-obama-administration-nixes-keystone-xl-pipeline-160930718--finance.html>

(National) Feds reject call for tougher fire-resistance for crude oil tank cars. The U.S. Department of Transportation announced November 10 that it is upholding its decision issued in the spring of 2014 to require new and retrofitted tank cars to be required to withstand being engulfed in a pool of burning liquid for 100 minutes without exploding, and rejected a call to toughen the fire-resistance of railroad tank cars that carry highly flammable crude oil. The department stated that 100 minutes was adequate time for first responders to assess the accident and evacuate the area. <http://www.chicagotribune.com/news/ct-crude-oil-tank-care-met-20151110-story.html>

INTERNATIONAL

(International) Paris attacks: 'France will destroy IS' – Hollande. France is committed to "destroying" the so-called Islamic State group after Friday's deadly attacks, President Francois Hollande has said. He said he would table a bill to extend the state of emergency declared after the attacks for three months and would suggest changes to the constitution. <http://www.bbc.com/news/world-europe-34836439>

(International) Islamic State threatens attack on Washington, other countries. Islamic State warned in a new video on Monday that countries taking part in air strikes against Syria would suffer the same fate as France, and threatened to attack in Washington. <https://ca.news.yahoo.com/islamic-state-threatens-attack-washington-other-countries-122051922.html>

(International)

(International) U.S. charges Scottish man over fake tweets that hurt stocks. The U.S. Department of Justice reported November 5 that a Scottish national was charged after he set up Twitter accounts as market research firms Muddy Waters Research and Citron Research and falsely reported that Audience Inc., and

UNCLASSIFIED

UNCLASSIFIED

Sarepta Therapeutics Inc., were under Federal investigation, sending their stock prices plunging and costing investors \$1.6 million in losses in an effort to profit from illegal trading.

<http://www.reuters.com/article/2015/11/06/us-usa-crime-tweets-idUSKCN0SV07G20151106>

(International) Security flaws found in Google Chromecast, Home Security Systems, Smart Coffee Makers. Security researchers from Kaspersky discovered several vulnerabilities in Internet of Things devices (IoT) including a “rickrolling” vulnerability in Google Chromecast devices that enables attackers to hijack smart TV content, a vulnerability in a smart coffee maker device that exposes the user’s Wi-Fi password, allowing attackers to spy on homeowners by connecting to Internet protocol (IP) cameras used in Webcams and baby monitors, as well as infiltrate a home security system by using powerful magnets that allows attackers to gain access to homes without triggering the alarm.

<http://news.softpedia.com/news/security-flaws-found-in-google-chromecast-home-security-systems-smart-coffee-makers-495864.shtml>

BANKING AND FINANCE INDUSTRY

(Nevada) Six charged in \$2.7 million tax refund fraud scheme. Federal authorities charged six people November 6 for their roles in a \$2.7 million Internal Revenue Service tax refund scheme where suspects would acquire the personal information of deceased persons from genealogical databases and use it to create fraudulent W-2 forms, driver’s licenses, and Social Security cards to file for tax refunds.

<http://www.news3lv.com/content/news/local/story/tax-refund-fraud-scheme-federal-Bogden/ozlX-4ppL0eIVnvHzVsHuA.cspX>

(International) Charges announced in J.P. Morgan hacking case. A Federal indictment was unsealed November 10 against three men in connection to an alleged massive cyber-attack against J.P. Morgan Chase & Co., and several other U.S. financial institutions that allowed the suspects to steal the personal information of more than 100 million customers by hacking into the financial institutions’ systems and stealing customer information to carry out a stock-

UNCLASSIFIED

manipulation scheme. The defendants would artificially inflate stock prices and send spam emails to customers to trick them into buying stocks.

<http://www.wsj.com/articles/prosecutors-announce-charges-in-connection-with-j-p-morgan-hack-1447169646>

(International) Treasury sanctions the Khanani Money Laundering Organization.

The U.S. Department of the Treasury's Office of Foreign Assets Control announced November 12 that the Altaf Khanani Money Laundering Organization (Khanani MLO) and Dubai-based money services company Al Zarooni Exchange were sanctioned as transnational criminal organizations after investigators determined that the organizations were knowingly laundering billions of dollars to organized crime groups, drug trafficking organizations, and designated global terrorist groups. <http://www.treasury.gov/press-center/press-releases/Pages/jl0265.aspx>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(National) Anhydrous Ammonia Facilities Prepare for New Federal Guidelines. Beginning in July there will be new federal guidelines for anhydrous ammonia facilities. The new OSHA policy change will require 275 of North Dakota's facilities to comply with their process safety rule.

<http://www.kxnet.com/story/30505890/anhydrous-ammonia-facilities-prepare-for-new-federal-guidelines>

COMMERCIAL FACILITIES

(Michigan) Four Winds warns of credit card breach. An official from Four Winds Casino Resort reported November 5 that its network system was compromised revealing cardholder names, card numbers, expiration dates, and internal verification codes for an unknown number of customers at its properties in New Buffalo, Hartford, or two facilities in Dowagiac following an investigation that found a program was installed onto the casino's network to search for payment card data from October 2014 – October 2015.

http://www.heraldpalladium.com/news/local/four-winds-warns-of-credit-card-breach/article_62ddc82a-64af-54e1-863c-b4052d000819.html

UNCLASSIFIED

(Virginia) Two men, one from Chester, accused of planning to shoot up or bomb churches and synagogues. Richmond officials reported that two men, associated with a white supremacy group, were charged for conspiracy to possess firearms after having been convicted of felonies, and another man charged with conspiracy to commit robbery November 9 after an undercover FBI investigation revealed that the men allegedly outlined plans to rob and kill a local silver/jewelry dealer, rob an armored car, and inflict harm on a gun store owner in an attempt to allegedly shoot or bomb churches and synagogues.

http://www.richmond.com/news/local/crime/article_7d8c76b3-5dd9-5365-a2c3-f0ac9682a989.html

COMMUNICATIONS SECTOR

(West Virginia) Cable theft disrupts Internet for thousands of customers.

Frontier Communications representatives reported November 5 that thieves seeking copper, cut fiber optic cables that caused 4,000 customers in McDowell County to experience an Internet and phone service outage that impacted 9-1-1 services. Officials are investigating the incident and crews restored service.

http://www.bdtonline.com/news/cable-theft-disrupts-internet-for-thousands-of-customers/article_d7aacd34-8433-11e5-a146-d76254738b77.html

(National) Comcast says it's not to blame after 200,000 user accounts were put up for the sale online. Comcast announced November 9 that it will reset passwords for roughly 200,000 customers after a package of personal data, including the e-mail addresses and passwords, was listed for sale for \$1,000 on a Dark Web site. The company reported it was not hacked and that its systems and apps were not compromised and held unsuspecting customers responsible for visiting malware-laden sites or fallen victim to other schemes that allowed hackers to obtain their data. <https://www.washingtonpost.com/news/the-switch/wp/2015/11/09/comcast-says-its-not-to-blame-after-200000-accounts-were-illegally-put-up-for-sale/>

(National) Securus Technologies: A rogue employee, not a hacker, exposed 70 million inmate calls. Securus Technologies announced November 12 that it is investigating an alleged breach of its systems that provides phone service to incarcerated people around the U.S., and stated that its system was not hacked

UNCLASSIFIED

UNCLASSIFIED

by an outside, but likely breached by an internal employee. An investigation into the breach, which reportedly includes unauthorized access to over 70 million recorded prison phone conversations, is ongoing.

<http://www.ibtimes.com/securus-technologies-rogue-employee-not-hacker-exposed-70-million-inmate-calls-2181819>

CRITICAL MANUFACTURING

(International) Mercedes-Benz recalls 126,000 vehicles over problems with airbags. Mercedes-Benz issued a recall November 4 for 126,000 model year 2008 – 2009 C300, C350, and C63 AMG vehicles, as well as 2010 GLK350 vehicles in the U.S. due to a malfunctioning control unit in its airbags that could cause them to improperly deploy in a crash or deploy immaturely. Mercedes has received at least 3 reports of inadvertent deployments in the U.S.

http://www.nytimes.com/2015/11/05/business/mercedes-benz-recalls-126000-vehicles-over-problems-with-airbags.html?_r=0

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(New Hampshire) Computer virus infects county dispatch center. The Strafford County chief deputy announced November 12 that computers at the Strafford County Regional Dispatch Center in Dover were infected by the CryptoLocker ransomware which severely limited the amount of data utilized by both dispatchers and emergency personnel on the field. Officials were able to isolate the virus and are working on bringing systems back online.

<http://www.fosters.com/article/20151112/NEWS/151119727>

UNCLASSIFIED

ENERGY

(Wisconsin) 2nd train derails in Wisconsin in 2 days, spills crude oil. Thirteen cars of an eastbound Canadian Pacific Railway train derailed and spilled less than 1,000 gallons of crude oil, and prompted evacuations of 35 homes in Watertown, Wisconsin, near the Mississippi River November 8. No fires or injuries were reported. <http://abcnews.go.com/US/wireStory/2nd-train-derails-wisconsin-days-spills-crude-oil-35057709>

(Wisconsin) Ethanol leaks into Mississippi River after train derailment. Five tanker cars of a BNSF Railway freight train derailed near Alma, Wisconsin, November 7 and leaked an unknown amount of ethanol into the Mississippi River, prompting the evacuation of 150 people and the closure of the railway and area highways while crews worked to clean the spill. <http://www.foxnews.com/us/2015/11/07/train-derails-in-wisconsin-prompting-voluntary-evacuation/>

(New York) Prosecutors allege persistent heating oil fraud in New York City. The Manhattan district attorney's office unsealed indictments November 10 against 44 people and 9 companies for allegedly stealing and reselling approximately \$34 million worth of oil that was never delivered to homeless shelters, hospitals, courthouses, police stations, and prison buildings on Rikers Island. The investigation uncovered 48 seized trucks that were rigged to deprive customers of their fuel, among several other fraudulent activities. <http://www.nytimes.com/2015/11/11/nyregion/11-indictments-detail-widespread-fraud-in-heating-oil-industry-of-new-york-city.html>

FOOD AND AGRICULTURE

(California) CDPH issues warning about Dungeness and Rock crabs caught in waters along the central and northern California coast. A statement released by the California Department of Public Health November 3 advised the public to avoid consuming Dungeness and Rock crabs caught in waters along the Oregon border and southern Santa Barbara county line until further notice due to high levels of domoic acid after State testing revealed that the toxin had consistently

UNCLASSIFIED

exceeded the State's action level. The advisory will be lifted once the amount of domoic acid returns to acceptable levels.

<http://www.cdph.ca.gov/Pages/NR15-082.aspx>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Massachusetts) Dad, son plead guilty in EBT scam. Two men pleaded guilty November 4 to stealing between \$1 million and \$1.5 million in food stamp benefits at their Lawrence bodega, Bonao Market, by charging customers paying with Electronic Benefit Transfer (EBT) for more than the items they purchased. The pair would then pocket a portion of the excess cash.

http://www.bostonherald.com/news/local_coverage/2015/11/dad_son_plead_guilty_in_ebt_scam

(Michigan) Three teens arrested in alleged school shooting plot at Linden community schools. Authorities arrested and charged 3 teenagers October 29 following an investigation into an alleged plot to carry out a school shooting at Linden Middle School and Linden High School in Michigan October 30. Police began an investigation after a school resource officer was given information on the alleged plot October 28.

http://www.mlive.com/news/flint/index.ssf/2015/11/three_teens_arrested_in_allege.html

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Updated Cryptowall encrypts file names, mocks victims. Researchers from both Bleeping Computer and an independent researcher discovered that the Cryptowall malware was recently updated to encrypt data on victims' machines and file names, making infected files difficult to recover without paying a ransom. The ransomware infects victims via email attachments, disguised as Microsoft Word documents, through JavaScript executable.

<https://threatpost.com/updated-cryptowall-encrypts-file-names-mocks-victims/115285/>

UNCLASSIFIED

(National) Fake IT admin tricked Cox rep into handing over customer database – cableco fined \$600K. The U.S. Federal Communications Commission fined Cox Communications for \$595,000 November 5 for allegations that the company failed to provide adequate security for its customer database and failed to notify the Federal government after a 2014 security breach in which a Lizard Squad hacker accessed customer records and leaked partial information on 8 customers and changed the passwords of 28 others while disguised as an employee in the Intelligence Technology (IT) department. The hacker had control over customer billing information including names, addresses, payment data, and even partial social security numbers and State identification numbers.

http://www.theregister.co.uk/2015/11/06/fcc_cox_data_breach/

(International) No surprise here: Adobe's Flash is a hacker's favorite target.

Researchers from Recorded Future released a new study November 9 revealing that Adobe Systems' Flash plugin was the highest targeted software program used by cybercriminals to install malware onto computers following research that revealed 8 of the 10 top vulnerabilities were seen targeting Adobe's Flash plugin.

http://www.computerworld.com/article/3003062/security/no-surprise-here-adobes-flash-is-a-hackers-favorite-target.html#tk.rss_security

(International) "Cherry Picker" PoS malware cleans up after itself. Researchers from Trustwave discovered that a point-of-sale (PoS) malware dubbed "Cherry Picker" relies on a new memory scraping algorithm using a file infector for persistence that removes all traces of the infection from the system with updated versions of sr.exe and srf.exe, which has been used to install the malware and inject a data definition language (DLL) into processes. The latest version of the malware relies on an application programming interface (API) called "QueryWorkingSet" to scrape the memory and harvest the data.

<http://www.securityweek.com/cherry-picker-pos-malware-cleans-after-itself>

(International) Latest Android phones hijacked with tidy one-stop-Chrome-pop.

A researcher from Quihoo 360 discovered, and reported during the MobilePwn2Own event at the PacSec security conference, a single clean exploit in Google's Chrome browser for Android via its JavaScript v8 engine that does not require several chained vulnerabilities to gain access and load software without user interaction once a user visits a malicious Web site.

http://www.theregister.co.uk/2015/11/12/mobile_pwn2own/

PUBLIC HEALTH

(Utah) Hepatitis C investigation expands to second hospital. Davis Hospital and Medical Center in Layton will notify 2,369 patients November 12 stating that they may have been exposed to hepatitis C after a patient at McKay-Dee Hospital contracted the blood-borne pathogen allegedly from a former nurse who stole morphine and Dilaudid. Davis Hospital issued alerts after investigators discovered that the nurse was previously employed and let go from the hospital for stealing intravenous Benadryl.

<http://www.deseretnews.com/article/865641401/Hepatitis-C-investigation-expands-to-second-hospital.html?pg=all>

TRANSPORTATION

(Texas) ABIA flight cancellations, delays could continue through Thanksgiving. Dozens of delays and cancellations continued at Austin-Bergstrom International Airport in Texas November 6 after heavy rains during the week of November 2 inundated the air traffic control tower at the airport and prompted the use of a temporary tower. The airport is expected to operate at less than half its normal capacity for several weeks due to flooding.

<http://kxan.com/2015/11/06/flight-cancellations-delays-continue-as-austin-airport-recovers-from-flooding/>

(California) Computer glitch leaves passengers stranded for hours after cruise ship arrives in San Pedro. A Princess Cruises spokesperson reported November 12 that 30 percent of the Star Princess's 2,600 travelers were temporarily stranded on the ship after docking in San Pedro, Los Angeles while crews manually processed passengers following a U.S. Customs and Border Protection computer failure. Officials reported that the incident was a result of a computer glitch and not a cyber-attack. <http://ktla.com/2015/11/12/computer-glitch-leaves-passengers-stranded-for-hours-after-cruise-ship-arrives-in-san-pedro/>

WATER AND DAMS

(Kentucky) ‘Code Red’ lifted after chlorine leak at Cynthiana water plant. A chlorine leak at a local water treatment plant prompted Cynthiana officials to evacuate a local Walmart and issue a ‘Code Red’ November 5 asking residents to stay indoors with their windows closed while crews worked to repair and assess the spill. No illnesses were reported.

<http://www.wkyt.com/home/headlines/Cynthiana-residents-asked-to-shelter-in-place-after-chlorine-leak-at-water-plant-341363132.html>

(South Carolina) DHEC issues repair orders for 167 more SC dams. The U.S. Department of Health and Environmental Control reported November 4 that an additional 167 dams have been requested for repairs in South Carolina following post-storm assessments by the U.S. Army Corps of Engineers after 75 dams ruptured in a historic October 4 storm. The requests require dam owners to submit a report with an engineer’s recommendations, as well as an application to receive a State permit for repairs by February 2, 2016.

<http://www.thestate.com/news/local/article43056084.html>

(Alabama) 10-year water leak in Cherokee finally repaired; should save town thousands. Officials reported November 9 that a 10-year leak that ran under U.S. 72 in Cherokee, Alabama, was finally repaired after workers from the Alabama Rural Water Association pinpointed the exact location of the leak using listening devices and other equipment, potentially saving the town tens of thousands of dollars. Officials estimated that 1.3 million gallons of water leaked per month over a period of 10 years costing the city approximately \$70,000 per year.

http://www.timesdaily.com/news/year-water-leak-in-cherokee-finally-repaired-should-save-the/article_d11a6960-15bc-5bf5-b2f9-22437aeb02f2.html

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165